

...from concept to acquisition

NAVAL WIRELESS NETWORKS SUMMIT

*Presented by:
Jesse Walker
Intel Corporation*

*Sponsored by: NETWARCOM and PEO ships
Hosted by: SPAWAR AND PEO C4I*

Why 802.11i?

- ***A world-wide interoperable standard***
 - ***Approved June 23rd***
 - ***Multi-vendor support***
 - ***Wi-Fi Alliance certification enforces interoperability***
- ***Verified security claims***
 - ***By industry, government, and academic researchers***
 - ***FIPS 140-2 Approved Algorithms***
- ***Cost/Performance sensitive design***

802.11i Operational Phases



Station



Access Point



Authentication Server



Security capabilities discovery



802.1X authentication



802.1X key management



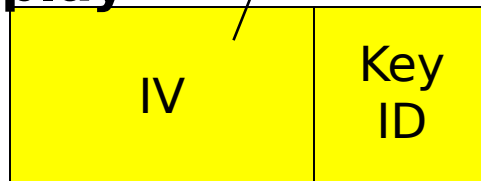
key distribution



Data protection

802.11i Data Protection

**IV used as frame
sequence space to defeat
replay**



**Cryptographic Message
Integrity Code to defeat
forgeries**



**encryption used to
provide data
confidentiality**